

EX PARTE OR LATE FILED

DEBEVOISE & PLIMPTON

555 13TH STREET, N.W.
WASHINGTON, DC 20004
(202) 383-8000

875 THIRD AVENUE
NEW YORK, NY 10022
TELEPHONE (212) 909-6000
TELECOPIER (212) 909-6836

21 AVENUE GEORGE V
75008 PARIS
TELEPHONE (33 1) 40 73 12 12
TELECOPIER (33 1) 47 20 50 82

INTERNATIONAL FINANCIAL CENTRE
25 OLD BROAD STREET
LONDON EC2N 1HQ
TELEPHONE (44 171) 786 9000
TELECOPIER (44 171) 588 4180

TELECOPIER: (202) 383-8118

February 3, 1999

13/F ENTERTAINMENT BUILDING
30 QUEEN'S ROAD CENTRAL
HONG KONG
TELEPHONE (852) 2810 7918
TELECOPIER (852) 2810 9828

BOLSHOI PALASHEVSKY PER.13/2
MOSCOW 103104
TELEPHONE (7-503) 956-3858
TELECOPIER (7-503) 956-3868

EX PARTE PRESENTATION

RECEIVED

FEB 11 1999

Ms. Magalie R. Salas, Esq.
Secretary
Federal Communications Commission
1919 M Street, NW, Room 222
Washington, DC 20554

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Carriage of the Transmissions of Digital Television Broadcast Stations – CS Docket No. 98-120

Dear Ms. Salas:

On Friday, January 29, 1999, the following representatives of the "5C" companies, (Hitachi, Ltd., Intel Corporation, Sony Corporation, Matsushita Electric Industrial Company, Ltd., and Toshiba Corporation)

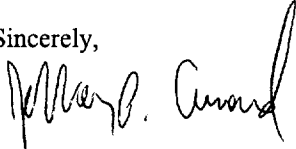
Jeffrey P. Cunard, Esq., Debevoise & Plimpton (representing Sony Corp.)
James Bonan, Vice President, Business Development, Sony Electronics Inc.
Brent Mori, Copyright Section, Legal and Intellectual Property Division, Sony Corp.
Christina Tellalian, Government Affairs, Sony Electronics Inc.
Seth Greenstein, Esq., McDermott, Will & Emery (representing Hitachi, Ltd.)
Michael Morazadeh, Intel Corp. (via phone)
Dr. Brendan Traw, Intel Corp. (via phone)
Peter Pitsch, Government Affairs, Intel Corp.
Sandra Aistars, Esq., Weil, Gotshal & Manges (representing Matsushita Electric Industrial Company, Ltd.)

met with the following members of the FCC staff:

Jon S. Wilkins, Director, Strategic Analysis, Office of Plans and Policy
Jonathan Levy, Staff Economist, Office of Plans and Policy
Mary Beth Murphy, Special Counsel, Office of General Counsel
Anita L. Wallgren, Legal Advisor, Office of Commissioner Susan Ness

We reviewed, discussed and responded to questions on the attached materials relating to content protection for digital television and the content protection system promoted by the 5C companies. In accordance with the FCC's rules, we are hereby filing two copies of this letter and the attached presentation materials.

Sincerely,


Jeffrey P. Cunard

Attachments

No. of Copies rec'd
List A B C D E

042

The following information was obtained from the records of the Department of the Interior, Bureau of Land Management, regarding the land owned by the United States in the State of California.

The following information was obtained from the records of the Department of the Interior, Bureau of Land Management, regarding the land owned by the United States in the State of California.



Policy Statements Regarding DTCP Adopters

January 26, 1999

As our industries move forward to deliver consumers compelling new digital content, protected over digital connections, several suggestions have been made on how the 5C DTCP system could be improved. Some of these suggestions have been based on sound business concerns, others based on mischaracterizations. To address these, the 5C companies and the DTLA provide a set of new policies and clarifications below.

These will be reflected in the next revision of the license agreements and related documents.¹

No Specification Modifications; Extended License Term

Once the 5C DTCP Specification reaches the 1.0 stage:

1. The Adopter Agreement's term shall be extended to ten years at the Adopter's option.
2. The DTCP Specification and Adopter Agreement covenants apply to the use of DTCP in all transports (1394, USB, RF, etc.) as each transport is mapped into the DTCP Specification.
3. Other than mapping the DTCP Specification onto new transports, the DTCP Specification shall not be materially revised, and the license (Adopter Agreement) shall not permit expansion of the licenses and covenants to new technical features.

The license provisions implementing these policies will give Adopters assurance that they will have ongoing access to the DTCP interface without placing their IP at risk and without backwards compatibility concerns.

Cost Shall Be Minimized

Once basic security levels for content are accomplished, the primary goal of the 5C is to have the lowest possible *total* cost of implementation. Therefore:

1. DTLA does not and shall not require the use of separate hardware components, such as smart cards (although smart card implementations of DTCP are permitted at the option of the manufacturer).
2. Fee levels are calculated to offset DTLA's costs. These fees shall not be increased unless DTLA's costs increase, and DTLA shall use commercially reasonable efforts to meet a price-reduction schedule.
3. Manufacturers making source-only devices, such as DVD players, and certain other devices, may avoid the fee and implementation expense of unique certificates by using a common 'send-only' certificate.

Revocation Shall Be Limited and Exercised Only With Due Process

Revocation is the capability of instructing DTCP-compliant devices not to release protected content to a limited list of certificates known to be compromised. This capability is required by the members of the MPAA as a condition of acceptance. Misuse of this capability would be harmful to the industry. Therefore:

1. Revocation shall only be used for
 - (a) specific cases of compromised keys, *i.e.*, where the key has been extracted from a licensed device and cloned into another device.
 - (b) response to cases of misdirection of keys.
 - (c) response to request of duly authorized governmental authorities.

¹ The Adopter Agreement, which includes the DTCP Specification and the Compliance Rules, are the actual legally-binding documents. The current version of the Adopter Agreement and Compliance Rules are available on DTLA's website at www.dtcp.com, and will be revised shortly to reflect the policies set out in this document. The Specification is available under an NDA, which is also on the website.

2. Revocation shall not (and can not) be used generally on a manufacturer's product line. The remedy of the content owners for general product design problems is as provided under the third-party beneficiary provisions of the Adopter Agreement. Revocation shall not be used for a general failure of DTCP technology or to remedy breaches of the Adopter Agreement.
3. The affected Adopter shall have notice and opportunity to object to proposed Revocation, together with the right to arbitrate the propriety of Revocation.

Adopters and Beneficiaries Participate in Process

Like other copy protection and other interface technologies, DTCP was developed as a private effort to meet an industry need. To bring this technology quickly to market with as few complications as possible, technical inputs were limited to companies who committed to license necessarily implicated IP under the Adopter Agreement. To better serve our "customers," the following provisions will be effective:

1. Amendments to the DTCP Specification are limited as described above.
2. An Adopters' Group is formed which will have the right to
 - participate in interoperability tests ("Plug Fests")
 - participate in ongoing discussions of the status of the DTCP system
 - review potential revisions to the Compliance Rules.
3. The existing "Content Participant Users Group" will continue in existence and will:
 - participate in ongoing discussions of the status of the DTCP system
 - have the right to initiate Revocations
 - review potential revisions to the Compliance Rules.

Compliance Rules Relate to Content Owner Requirements

The general and detailed requirements of the Compliance Rules have been negotiated over a period of years with the content owners. Virtually the same requirements are found in the CSS license. In general, the Compliance Rules contain requirements that limit a licensed product as follows:

- Internal copying of protected content is prohibited or regulated.
- Outputs to other devices are limited to certain digital and analog media from which copying is reasonably difficult.
- The product should be designed so that its copy-protection features are quite difficult to circumvent.

No requirement that adds cost or material complexity to product implementations is or shall be included in the Compliance Rules except to address the copy protection requirements of the content owners. To simplify manufacturers' use of the Compliance Rules, DTLA is preparing a revision which clarifies which rules apply to which types of devices.²

Adopters Shall Receive Truthful Information About DTCP

There have been many conflicting statements about 5C and other technologies. It is the policy of DTLA and its member companies to conduct their businesses with uncompromising integrity. In addition to points covered above, we provide clarifications on certain points which have been the subject of confusion.

Export

DTCP-compliant products are freely exportable from the U.S. and Japan. In the US, for example, we have received a "Commodity Classification" from the U.S. Department of Commerce, permitting export.

Authenticating Information in Devices

Keys and certificates, or other non-exposed information, are needed in licensed products to avoid trivially simple piracy which would be enabled by implementing a public interface in a non-compliant (copying) device.

² Adopters may, at their option, follow the "Procedural Specification" of the CSS agreement in lieu of following the "Compliance Rules" of the DTCP Adopter Agreement. In some cases, this may reduce design cycles and costs.

Response of 5C to the

Consumer Electronics Manufacturers Association

R4.8 Subcommittee Working Group 2

Call for Information

Hitachi, Ltd.
Intel Corporation
Matsushita Electric Industrial Co., Ltd.
Sony Corporation
Toshiba Corporation

December 4, 1998

Table of Contents

	<u>Page</u>
Preface	iii
Section 1. Detailed Summary of the Proposal	1
Section 2. Key Management	8
Section 3. Implementation	13
3.1 CE Hardware Implementation	13
3.2 CE Software Implementation	14
Section 4. Robustness of Each Cryptographic Algorithm	15
4.1 Encryption	15
4.2 Authentication	15
4.3 Hashing	16
4.4 Digital Signature	16
Section 5. Error Propagation Characteristics of the Encryption Algorithms	17
Section 6. Renewability	18
Section 7. Making Legitimate Copies	22
Section 8. Resistance to Obsolescence	25
Section 9. Maintenance Complexity	26
Section 10. Applicability to Different Digital Interfaces	27

Section 11. Availability for Import and Export	28
Section 12. Licensing Terms	29
Section 13. Licensable Intellectual Property	30
Section 14. Circumvention Devices	31
Section 15. Amendments Needed to Interface Standards	33
Section 16. View of 5C Regarding Standardization of Copy Protection	34
Section 17. Other Information	36

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Hitachi, Ltd., Intel Corporation, Matsushita Electric Industrial Co., Ltd., Sony Corporation, and Toshiba Corporation (the "5C") disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. Implementation of the elements of the 5C DTCP system described herein requires a license from the Digital Transmission Licensing Administrator. The Digital Transmission Licensing Administrator can be contacted at dtla-manager@dtcp.com. The URL for the Digital Transmission Licensing Administrator web site is: <http://www.dtcp.com>.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein. This document responds to particular questions propounded at a particular point in time, and is subject to change without notice.

Copyright © 1997, 1998 by Hitachi, Ltd., Intel Corporation, Matsushita Electric Industrial Co., Ltd., Sony Corporation, and Toshiba Corporation. Third-party brands and names are the property of their respective owners.

Section 1. Detailed Summary of the Proposal

As members of the Digital Transmission Discussion Group ("DTDG") of the Copy Protection Technical Working Group ("CPTWG"), Hitachi, Intel, Matsushita (MEI), Sony and Toshiba jointly produced the Five Company ("5C") Digital Transmission Content Protection ("DTCP") Specification, providing a simple and inexpensive method affording a high degree of protection for copyrighted commercial entertainment content transmitted over bidirectional digital interfaces.

The 5C DTCP Specification defines a cryptographic protocol for protecting audio/video entertainment content from unauthorized copying, intercepting and tampering as it traverses high performance digital interconnects. Only legitimate entertainment content delivered to a source device via another approved copy protection system (including but not limited to the Content Scrambling System used for DVD Video ("CSS") and conditional access systems used for digital cable and satellite video transmissions) will be protected by this system.

The 5C DTCP Specification relies on strong cryptographic technologies to provide flexible and robust copy protection. These cryptographic techniques have evolved over the past 20 years to serve critical military, governmental, and commercial applications. They have been thoroughly evaluated by legitimate cryptographic experts and hackers, and have proven their ability to withstand attack. The cryptographic stability of the system is derived from the proven strength of the underlying technologies, rather than merely how well a certain algorithm can be kept secret.

The 5C DTCP Specification enables these powerful encryption and authentication techniques to be implemented without imposing heavy burdens on consumer electronics devices. Manufacturers of typical CE devices can easily implement the 5C DTCP Specification without adding significant design complexity or manufacturing or product cost. Notably, the 5C DTCP system also imposes little burden upon information technology companies that wish to incorporate the system in their products, or upon motion picture and recording companies that wish to use the 5C DTCP system to protect transmissions of their content.

The 5C DTCP system further was designed to coexist with current copy protection technologies, such as CSS and conditional access systems for digital television transmission, and to be compatible with other content encryption and watermarking technologies developed in the future.

A number of emerging technologies will take advantage of the high speed digital interfaces, including desktop computers, DVD players, digital televisions and digital set-top-box receivers. The transparent 5C DTCP framework allows consumers to use these devices to enjoy high-quality digital pictures and sound without any noticeable performance or quality impact.

In this Response, the 5C sets forth specific examples of the 5C DTCP system as implemented for the IEEE 1394 interface standard. The 5C DTCP system initially was designed for the IEEE 1394 interface, in accordance with the terms of the CPTWG DTDG Call for Proposals. However, the 5C DTCP system can readily be applied to other interfaces as well, in particular to any high-speed bidirectional interface.

1394 Content Protection Architecture

Content Protection Layers

The 5C DTCP system addresses four fundamental layers of content protection:

- Authentication and key exchange
- Content encryption
- Copy control information
- System renewability

Each of these layers is discussed below in a brief overview, and in greater detail in the remaining sections of this Response.

Authentication and Key Exchange (AKE)

Before sharing valuable information, a connected device must first verify that another connected device is authentic. In an effort to balance the protection requirements of the film and recording industries with the real-world requirements of PC and CE users, the specification includes two authentication levels - Full Authentication and Restricted Authentication.

- **Full Authentication** can be used with all content protected by the system, and must be used for copy-never content.
- **Restricted Authentication** enables the protection of copy-one-generation and no-more-copies content. If a device handles either copy-one-generation or no-more-copies protection schemes, the device must support restricted authentication. Copying devices, including consumer electronics devices such as digital videocassette recorders, DVD recording devices, and D-VHS recorders and devices communicating with them, employ this kind of authentication and key exchange.

No authentication is performed for content that may be copied without restriction.

Table 1 illustrates the authentication method performed, based on the source and sink device authentication capabilities:

Source	Sink	Authentication Performed
Full	Full	Full
Full	Full / Restricted	Full
Full / Restricted	Full	Full
Full / Restricted	Full / Restricted	Full
Full / Restricted	Restricted	Restricted
Restricted	Full / Restricted	Restricted
Restricted	Restricted	Restricted
Full	Restricted	None ¹
Restricted	Full	None ¹

Table 1. Authentication Method Matrix

Both Full and Restricted Authentication involve the calculation of three types of keys:

- an **authentication key**, established during authentication, used to encrypt the exchange key;
- an **exchange key** used to set up and manage the security of copyrighted content streams; and,
- a **content key** used to encrypt the content being exchanged.

When executing AKE, various information should be exchanged using 1394 asynchronous packets between source and sink devices. This mechanism of exchange using asynchronous 1394 packets is based upon the IEC-61883 specification and the AV/C Digital Interface Command Set. The 5C also believe that these mechanisms fully comply with the EIA-775 Interface for IEEE 1394. The necessary extensions to these specifications are described in detail in the 5C DTCP Specification and have already been adopted by the relevant bodies, including the 1394TA AV/C working group.

Content Encryption

The content cipher, that is, the algorithm used to encrypt the digital content itself, must be robust enough to protect the content yet efficient enough to implement in PCs and CE devices. To ensure interoperability, all devices must support the cipher specified as the baseline cipher. The channel cipher subsystem can also support additional ciphers, the use of which is negotiated during authentication. All ciphers are used in the

¹ Protected content cannot be exchanged in these circumstances.

converted cipher block chaining mode. Converted cipher block chaining provides greater security than ordinary cipher block chaining.

The 5C DTCP Specification requires Hitachi's M6 as the baseline cipher. The M6 cipher is a common-key block cipher algorithm based on permutation-substitution. This rotation-based algorithm works the same way as encryption algorithms currently used in Japanese digital satellite broadcasting systems.

Optional, additional ciphers include the Modified Blowfish cipher and the Data Encryption Standard (DES) cipher.

The Content Cipher Subsystem must be able to support the bandwidth of an MPEG-2 compressed video stream. For PCs, this cipher subsystem may be implemented in software. Software M6 encryption/decryption of a 64 KB block of data as tested on a 266-MHz Pentium® II Processor, had an approximate bandwidth of 200 Mbps.

For CE devices, the M6 channel cipher will typically be implemented in hardware. About 6K gates are estimated to be required for a 10-round M6 with C-CBC hardware implementation. This implementation is capable of encryption or decryption at 32 Mbps with a 25-MHz clock.

Copy Control Information (CCI)

Content owners need a way to specify whether their content can be duplicated. The content protection system must therefore support transmission of encrypted data between devices, using **Copy Control Information (CCI)**. If source and sink devices have conflicting capabilities, they should follow the most restrictive CCI method(s) available, which is determined by the source device. Two methods can be used:

- The **Encryption Mode Indicator (EMI)** provides easily accessible yet secure transmission of CCI via the most significant two bits of the synch field of the isochronous packet header. The encoding used for the EMI bits distinguishes the content encryption/decryption mode: copy-freely, copy-never, copy-one-generation, or no-more-copies.
 - No authentication or encryption is required to protect content that can be copied freely.
 - Content that is never to be copied (e.g., content from prerecorded media with a Copy Generation Management System ("CGMS") value of 11, such as a DVD Movie) can only be exchanged between devices that have successfully completed full authentication.
 - Content that can be copied one generation (e.g., content with a CGMS value of 10, such as a pay TV program) can be exchanged between devices using either full or restricted authentication.

- For content marked no-more-copies, future exchanges are marked to indicate that a single-generation copy has already been made. This content can be exchanged between devices using either full or restricted authentication.

By locating the EMI in an easy-to-access location, devices can immediately determine CCI without needing to extract embedded CCI (e.g., in the MPEG transport stream). This ability is critical for bitstream recording devices (such as a digital VCR) that do not recognize and cannot decode specific content formats. When multiple mechanisms are available, the most restrictive should be used. The EMI indicates the mode of encryption applied to a stream:

- Source devices will choose the right encryption mode based on embedded CCI and set the EMI accordingly.
- Sink devices will choose the right decryption mode by examining the EMI.

If the EMI bits are tampered with, the encryption and decryption modes will not match, resulting in erroneous decryption of the content.

- **Embedded CCI** is carried as part of the content stream. Many content formats including MPEG have fields allocated for carrying the CCI associated with the stream. The integrity of embedded CCI is ensured since tampering with the content stream results in erroneous decryption of the content. Only devices capable of processing the content itself can process this form of CCI.

System Renewability

Devices that support full authentication can receive and process **System Renewability Messages (SRMs)**. These SRMs are generated by the Digital Transmission Licensing Administrator (DTLA) and delivered via content and new devices. System renewability ensures the long-term integrity of the system and provides the capability for revoking unauthorized devices.

- Prerecorded content source devices such as DVD players should be able to update an SRM from prerecorded content media (such as a DVD disc). In addition, prerecorded content should carry a system renewability message current as of the time the content is mastered. Such devices should also be able to update an SRM from another compliant device with a newer SRM.
- Devices such as a digital set-top boxes (“STB”) serving as digital cable receivers or DBS digital broadcast satellite receivers are a real-time delivery source of copyrighted content. They should be able to update an SRM from content stream or from another compliant device with a newer SRM.
- Devices such as digital televisions are a receiver of copyrighted content. These devices should be able to update an SRM from another compliant device with a newer SRM.

- Devices such as DV recorders are a format-cognizant recording and playback device. Other recording devices such as D-VHS are a format-non-cognizant recording and playback device. SRM support by these devices is only necessary if they support prerecorded copyrighted content marked copy-never. Thus, full authentication is used. If SRM support is required, both types of devices should be able to update an SRM from another compliant device with a newer SRM.

Typical Device Components

Figure 1 shows the components typically required for a device to be compliant with digital transmission content protection, as applicable to the IEEE 1394 interface.

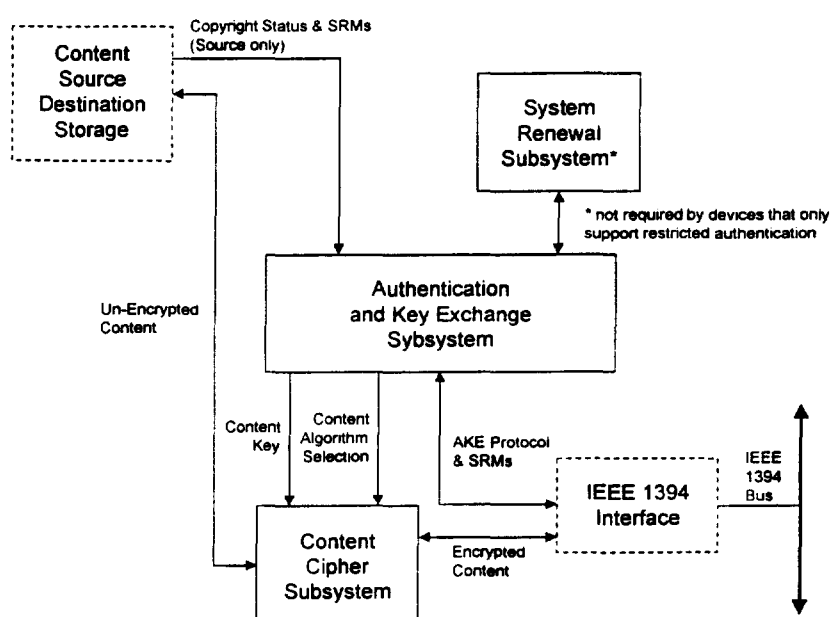


Figure 1. Typical Components of a Compliant Device

Subsystems in boxes with solid outlines are required for compliance. Boxes with dashed outlines are subsystems common to compliant and non-compliant devices. Depending on the device class, it will interact with a content source, a content destination, or content storage. For example, source devices receive content source. display devices send content to a destination, and recording and playback devices store content on media such as tape. Components include:

- An **Authentication and Key Exchange (AKE) Subsystem** for performing full or restricted authentication;
- A **Content Cipher Subsystem** for handling encryption/decryption of copyrighted content after authentication; and,

- **System Renewal Subsystem** for supporting the system renewability mechanism associated with full authentication. The newest version of the SRM is stored here.

A robust **Random Number Generator (RNG)** is required for use as needed during authentication. For CE devices, the authentication and key-exchange mechanisms can be implemented in software running on an embedded micro-controller. To increase CE device performance, cryptographic acceleration hardware can be added. Currently, it is anticipated that the channel ciphers would be implemented in hardware. On a PC, the system can be implemented entirely in software. All implementations of this content protection system must be tamper-resistant.

Section 2. Key Management

Full Authentication

Full Authentication can be used with all content protected by the system, and must be used for copy-never content. The Full Authentication protocol employs the public-key-based Digital Signature Algorithm (DSA) algorithm and the Diffie-Hellman (DH) key-exchange algorithm. Both the DSA and Diffie-Hellman implementations for the system employ Elliptic Curve (EC) cryptography. This technique offers superior performance compared to systems based on calculating discrete logarithms in a finite field.

EC-DSA is a method for digitally signing and verifying the signatures of digital documents to verify the integrity of the data.

EC-DH key exchange is used during Full Authentication to establish a shared authentication key (K_{Auth}).

Figure 2 gives an overview of the Full Authentication protocol flow.

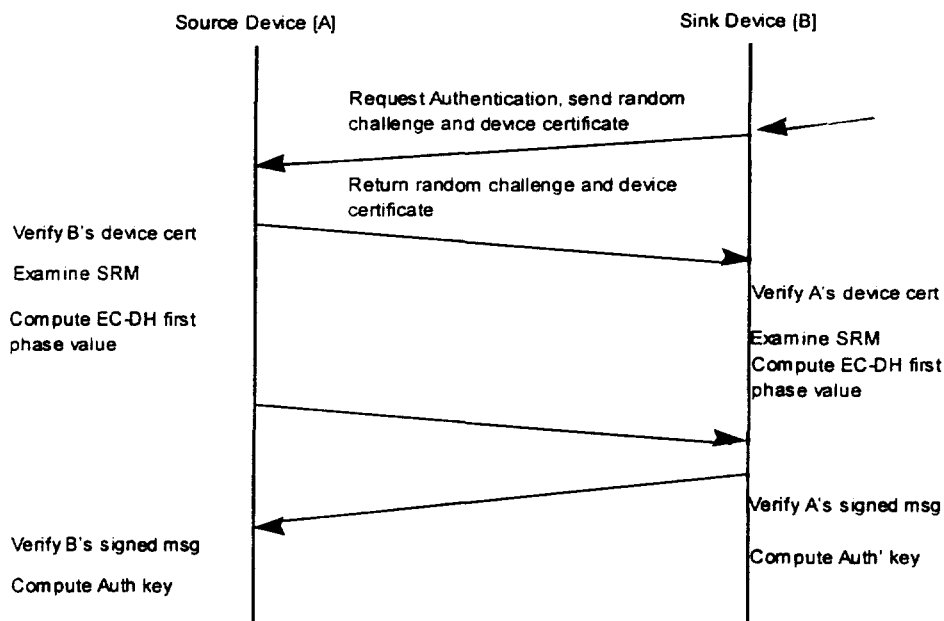


Figure 2. Full Authentication Protocol Flow Overview

A detailed description of the Full Authentication protocol and associated state machines can be found in the 5C DTCP Specification available under a nondisclosure agreement ("NDA") from the DTLA.

The following keys are associated with Full Authentication:

Key	Size (bits)
DTLA Public Key	320
Device Private Key	160
Device Public Key	320

Please note that each device requires an unique public/private key pair and device certificate assigned by the DTLA. The Device Private Key must be securely stored in the device.

Restricted Authentication

Restricted authentication is an AKE method for devices with limited computing resources. This method can be used by copying devices (such as DV recorders or D-VHS recorders) and devices communicating with them for authenticating copy-one-generation and no-more-copies contents.

Authentication is based on each device receiving a small, relatively unique² set of secret keys from the DTLA. These secret keys are derived from a much larger set of secrets which are generated and maintained by the DTLA. During Restricted Authentication, these keys are combined in a manner determined by the other device's key selection vector to establish a common verification key. This verification key is used for authentication as well as computing a common Authentication Key (K_{Auth}).

² It is unlikely that any two devices will have the same set of secrets.

Figure 3 gives an overview of the Restricted Authentication protocol flow.

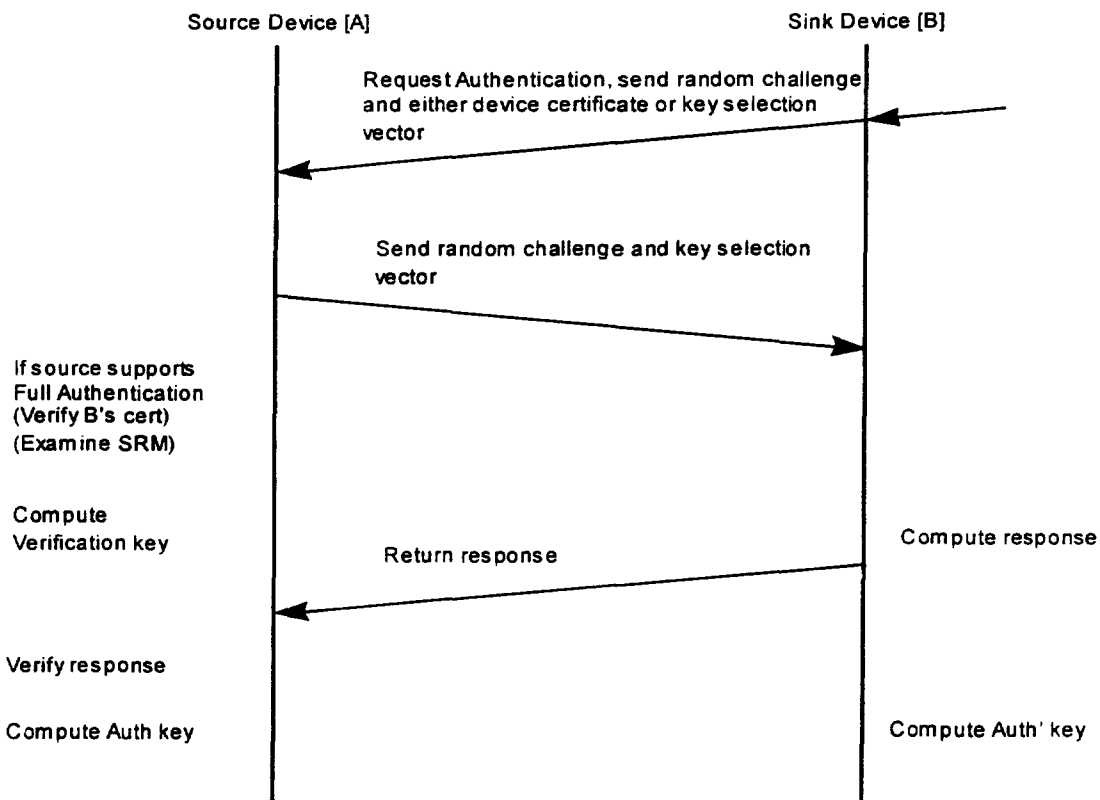


Figure 3. Restricted Authentication Protocol Flow Overview

A detailed description of the Restricted Authentication protocol and associated state machines can be found in the 5C DTCP Specification available under NDA from the DTLA.

The following keys are associated with Restricted Authentication:

Key	Size (bits)
"Copy-one-generation" Sink Device Keys ($X_{Kcosnkl} \dots X_{Kcosnkn}$)	64 (Each)
"Copy-one-generation" Source Device Keys ($X_{Kcosrcl} \dots X_{Kcosrcn}$)	64 (Each)
"No-more-copies" Sink Device Keys ($X_{Knmsnkl} \dots X_{Knmsnkn}$)	64 (Each)
"No-more-copies" Source Device Keys ($X_{Knmsrcl} \dots X_{Knmsrcn}$)	64 (Each)

Please note that all of these keys are not required in every device. For instance, a digital VCR would only need $X_{Kcosnkl} \dots X_{Kcosnkn}$ and $X_{Knmsrcl} \dots X_{Knmsrcn}$. These keys must be securely stored in the device. Each device requires a set of keys assigned by the DTLA and a unique device certificate.

Exchange Key (K_X)

A common set of **Exchange Keys** (K_X) are established between a source device and all sink devices that have completed the appropriate authentication procedure (either Full or Restricted) with the source device required to handle content with a specific EMI value. In addition, if optional content ciphers³ are mutually supported, Exchange Keys are established for use with them for Copy-Never content.

Exchange keys are protected during establishment by K_{Auth} .

Content Key (K_c)

The **Content Key** (K_c) is used as the key for the content encryption engine. K_c is computed from the three values shown below:

- Exchange Key K_X assigned to the EMI and cipher/key length being used to protect the content.
- A random number N_c generated by the source device and is sent in plain text to all sink devices. Constant value C_a , C_b , or C_c , which corresponds to the encryption mode indicator.

The Content Key is generated as follows:

$$K_c = J[K_X, N_c, f[EMI]] \quad \text{where: } \begin{aligned} f[EMI] &= C_a \text{ if EMI is mode A} \\ f[EMI] &= C_b \text{ if EMI is mode B} \\ f[EMI] &= C_c \text{ if EMI is mode C} \end{aligned}$$

C_a , C_b , and C_c are universal secret constants assigned by the DTLA. The values for these constants are specified in 5C DTCP Specification available under license from the DTLA. The definition of function $J[]$ is also described in this document.

Periodically, the source device shall change Content Keys to maintain robust content protection. The maximum period is defined as 120 seconds. Duration time for K_c is from 30 seconds to 2 minutes.

Key Sizes

The lengths of the keys and constants described above are set forth in the following Table 2:

³ Only applicable for Exchange Keys established as a result of Full Authentication between devices which both support the optional capability mask in the device certificate.

Key, Variable, or Constant	Size (bits)
Exchange Keys (K_x)	96
Scrambled Exchange Keys (K_{sx})	96
Constants (C_a, C_b, C_c)	24
Content Key for Baseline Cipher (K_c)	56
Content Key for Optional Ciphers ⁴ (K_c)	56 – 64
Nonce for Content Channel (N_c)	64

Table 2. Length of Keys and Constants (Content Channel Management)

⁴ Features of the specification that are labeled as “optional” describe capabilities whose usage has not yet been established by the DTLA.

Section 3. Implementation

The initial implementation of the 5C DTCP Specification is designed for use via the IEEE 1394 interface. Such interfaces commonly will be used in a variety of digital consumer electronics and personal computing devices, as well as in home network communications. The 5C DTCP Specification does not impose a particular mandatory method of implementation. Device designers have substantial flexibility in determining the most efficient way of complying with the Specification, including rules regarding compliant operation and robustness of design against circumvention.

Somewhat different requirements are imposed upon devices that act solely as sources of content, such as Digital Set Top Boxes and Digital Video Disk Players; devices that act solely as sinks for content, such as Digital TV display devices; and devices that are likely to be both sources and sinks, such as Digital Video Recorders. Source devices require the ability to perform authentication and to encrypt content to be transmitted via 5C. Sink devices are required to perform authentication and to decrypt content. Devices that act as both sources and sinks will be required to perform authentication and to both encrypt and decrypt content. Moreover, CE sink devices that are capable of recording content likely will perform Restricted Authentication, which reduces the hardware requirements on CE devices and improves speed and performance of authentication.

3.1 CE Hardware Implementation

For CE devices, the M6 channel cipher will typically be implemented in hardware. About 6K gates are estimated to be required for a 10-round M6 with C-CBC hardware implementation. More particularly:

- Registers and Sizes: approximately 429 bits total (3432 gates)
- Arithmetic functions (number, size and definition): 2 32-bit ADDERS, 88 2 input XORS (712 gates)
- RAM, ROM, NVRAM, FIFO: 0
- Miscellaneous logic: 240 2 input selectors, 64 3 input selectors, 64 input selectors (approximately 2030 gates)
- Total Gate Count: Approximately 6174 gates
- Performance: This implementation is capable of encryption or decryption at 32 Mbps with a 25-MHz clock.

Other elements of the system may be implemented in or assisted by hardware, at the discretion of the manufacturer.

The 5C DTCP development team includes design, manufacturing and security engineers from among the world's foremost consumer electronics and information technology companies. The 5C designed the 5C DTCP system for ease of implementation in both consumer electronics and information technology devices. Implementations of the 5C DTCP system do not require expensive components or

external devices. All essential functions of the 5C DTCP Specification can be carried out in multi-function semiconductor devices at a very low cost. The DTLA has received expressions of interest in the 5C system from numerous prominent semiconductor manufacturers. The 5C therefore anticipate that more than a sufficient number of vendors will make available semiconductor devices that incorporate 5C DTCP functions, thereby providing an inexpensive, flexible and easy-to-implement method of content protection to manufacturers of any CE device.

3.2 CE Software Implementation

All elements of the 5C DTCP system not implemented in hardware will be implemented using embedded firmware. If desired, however, all elements of the system could be implemented in software.

As noted, M6 encryption and decryption is likely to be performed in hardware in CE devices. In a typical implementation, the authentication and key exchange algorithms and protocols will be implemented in software. The approximate resource requirements and performance for these functions on a 32 bit processor commonly found in CE devices is as follows:

Authentication Type	Performance	Program Size
Restricted	30 mS	5 KB
Full	1 S	20 KB

Section 4. Robustness of Each Cryptographic Algorithm

The 5C DTCP system uses algorithms and authentication means that have passed rigorous laboratory testing and have proven to be robust in numerous commercial applications, including applications that are similar to the transmission of copyrighted content. There are no known structural weaknesses to any of the cryptographic algorithms used in the 5C DTCP system. It is estimated that a known plain text attack would require greater than 2^{55} operations in a key exhaustive search, and a greater number of operations would be required in case of a chosen plain text attack.

4.1 Encryption

The Hitachi M6 algorithm is used with 56-bit keys in the 5C DTCP system. This algorithm has been deployed in commercial satellite television transmission systems in Japan for several years. Before selecting the M6 algorithm as the baseline cipher for the 5C DTCP system, the algorithm was independently evaluated by encryption experts from each of the 5C companies, and was believed to be robust against reasonably foreseeable types of attacks. The M6 algorithm also has proven to be robust in the field and to our knowledge it has not been hacked or otherwise successfully circumvented. As a general matter, 56-bit encryption implementations have proven robust in commercial applications. Extreme computational power, time and expense would be required to crack a 56-bit algorithm. A brute force attack likely would require the type of computing capabilities currently found only in highly advanced research laboratories, and would be far in excess of the computing power that is anticipated to be accessible to consumers for the foreseeable future.

4.2 Authentication

The Authentication and Key Exchange is performed using the public key Elliptic Curve Digital Signature Algorithm (EC-DSA) for signing and verification, and the Elliptic Curve Diffie-Hellman (EC-DH) key exchange algorithm to generate a shared authentication key. Public key cryptography has been successfully employed over the last two decades in a variety of contexts in digital networks requiring secure transmissions and privacy of communications. These methods are compatible with industry standards (such as IEEE P1363) for key exchange and authentication in a digital network environment, including implementations for personal computing devices. These methods were selected for use in the 5C system by experts in the field of encryption in each of the 5C member companies, based on their knowledge of the robustness of these methodologies in the field and the rigorous testing these methods have passed over the last two decades. Again, the 5C is unaware of any instances in which these technologies have been proved to be susceptible to attack or circumvention in commercial application. Extreme computational power, time and expense have been applied in attempts to defeat elliptic curve cryptography, to no avail. Even brute force attacks using the type of computing capabilities currently found only in highly advanced research laboratories have been unsuccessful.

4.3 Hashing

SHA-1, as described in FIPS PUB 180-1⁵ is the algorithm used in DSS to generate a message digest of length 160 bits. A message digest is a value calculated from message. It is similar in concept to a checksum, but computationally infeasible to forge.

4.4 Digital Signature

The Authentication and Key Exchange is performed using the Elliptic Curve Digital Signature Algorithm (EC-DSA) for signing and verification. These cryptographic algorithms are based upon cryptographic schemes, primitives, and encoding methods described in IEEE P1363/D3 (May 11, 1998). The IEEE P1363/D3 is an unapproved draft that is subject to change. Changes may occur in subsequent versions of that draft that interfere with conformance to the final IEEE 1363 standard of the cryptographic algorithms described herein.

Elliptic curve digital signature methods are well known and in widespread commercial use in the computer industry for applications requiring robust and secure implementations. The 5C system-specific EC-DSA system will be robust against MOV reduction attack, since super singular elliptic curves are avoided.

⁵ National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)," FIPS Publication 180-1, April 17, 1995.

Section 5. Error Propagation Characteristics of the Encryption Algorithms

Error propagation within a packet may result in loss of the corresponding source packet, with a probable impact upon one block (64 total bits) and a maximum of two blocks (128 total bits).

Section 6. Renewability

Compliant devices that support Full Authentication can receive and process system renewability messages (SRMs) created by the DTLA and distributed with content. These messages are used to ensure the long-term integrity of the system.

SRM Message Components and Layout

There are several components to a system renewability message (SRM):

- A message **Type** field (4 bits). This field has the same encoding as is used for the certificate type field in device certificates. The only encoding currently defined is 0, which indicates that the message is for IEEE 1394 content protection.
- A message **Generation** field (SRMM) (4 bits). This field specifies the generation of the SRM. It is used to ensure the extensibility of the SRM mechanism. Currently, the only encoding defined is 0, indicating a first generation SRM with a maximum size as specified in the 5C DTCP Specification available under license from the DTLA. Other encodings are currently reserved. This value remains unchanged even if only part of the SRM can be stored by the device (e.g., $X_{SRMC} \leq SRMM$).
- Reserved field (8 bits). These bits are reserved for future definition and are currently defined to have a value of zero.
- A monotonically increasing system renewability message **Version Number** (SRMV) (16 bits). This value is exchanged as X_{SRMV} during Full Authentication. This value is not reset to zero when the message generation field is changed.
- **Certificate Revocation List (CRL) Length** (16 bits). This field specifies the size (in bytes) of the CRL including the CRL Length Field (2 bytes), CRL Entries (variable length), and DTLA Signature (40 bytes).
- **CRL Entries** (variable sized). The CRL used to revoke the certificates of devices whose security has been compromised. Its format is described in the following section.
- The **DTLA EC-DSA signature** of these components using L^{-1} (320 bits).

The structure of first-generation SRMs is shown in Figure 4. The fields in the first 4 bytes of the SRM comprise the SRM Header.

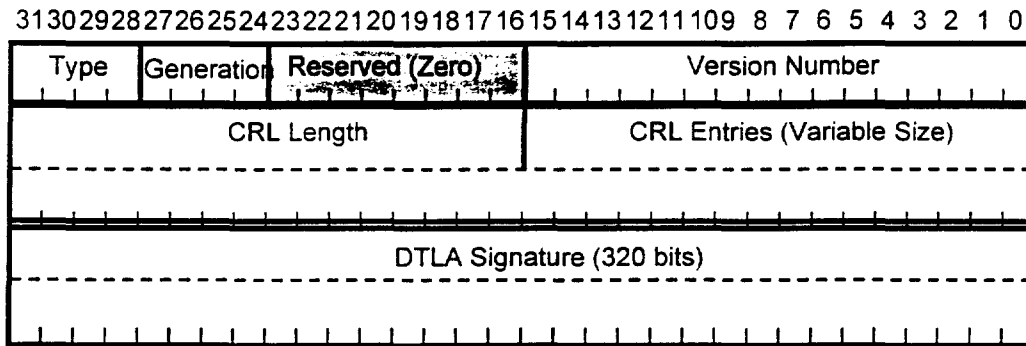


Figure 4. Structure of the First-Generation System Renewability Message

Certificate Revocation List

The **Certificate Revocation List (CRL)** identifies devices that are no longer compliant. It consists of the CRL Length field that specifies the length of the CRL in bytes. This field is followed by a sequence of entry type blocks (1 byte) which are in turn followed by the number of CRL entries specified by the entry type block. Two types of entry block are supported. One type provides for the revocation of individual devices while the second allows for the revocation of blocks of up to 65535 devices.

DTLA EC-DSA Signature

The DTLA EC-DSA signature field is a 320-bit signature calculated over all of the preceding fields of the SRM using the DTLA EC-DSA private key L^{-1} . This field is used to verify the integrity of the SRM using the DTLA EC-DSA public key L^1 .

SRM Scalability

To ensure the scalability of this renewability solution, the SRM format is extensible. Next-generation extensions (CRLs and possibly other mechanisms) to a current-generation SRM format must be appended to the current-generation (as shown below in Figure 5) in order to ensure backward compatibility with devices that only support previous-generation SRMs. Devices are only responsible for supporting the generation of SRM that was required by the DTLA as of the time the device was manufactured. The conditions under which the DTLA will authorize new-generation SRMs are specified in the DTLA license agreement.

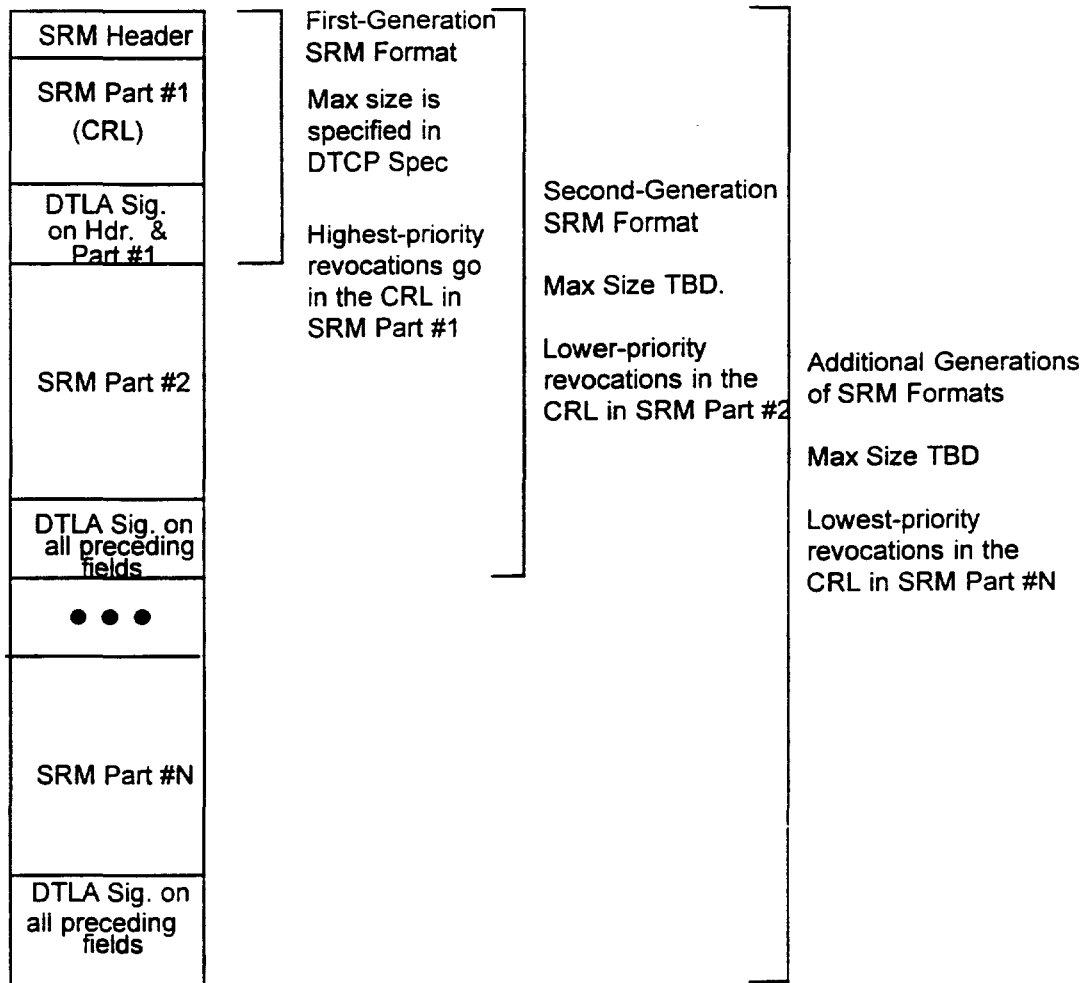


Figure 5. SRM Extensibility

Updating SRMs

System renewability messages can be updated from:

- other compliant devices (connected via the digital transmission means) that have a newer list;
- prerecorded content media; and,
- content streams via real-time compliant devices that can communicate externally (e.g., via the Internet, phone line, cable system, direct broadcast satellite, etc.).

The general procedure for updating SRMs is as follows:

1. Examine the version number of the new SRM.
2. Verify that the SRM version number is greater than the one stored in non-volatile storage.
3. Verify integrity with the DTLA public key (L^1).
4. If SRM is valid and new, then store as much as will fit of the newer version of the message in the device's non-volatile storage.

The 5C DTCP Specification provides effective renewability that will ensure long-term viability of the 5C DTCP system. Moreover, the DTLA license conditions assure that revocation will be undertaken only as absolutely necessary to protect the integrity of the system. Content owners cannot unilaterally revoke device certificates. The DTLA will create an SRM only when presented with clear evidence that a certificate has been lost or stolen, or else utilized by unauthorized sink devices for purposes of circumventing the 5C DTCP system. These conditions assure that manufacturers and consumers will not have their legitimate devices unfairly revoked. The DTLA license also provides a process for review of revocation decisions, such that any device that wrongfully has been revoked may be reactivated through an updated SRM.

Section 7. Making Legitimate Copies

The 5C DTCP system permits the making of legitimate copies of content according to the setting of Copy Control Information that is required to be included as the EMI. Settings are provided so as to indicate that content may be copied with no restriction against further copying, or that one generation of copies may be made from the transmitted content.

When the EMI indicates that CCI has been set so as to indicate that copying shall not be inhibited, the 5C DTCP protocol requires that the 5C system should not be employed, and that content should be sent without 5C encryption or authentication.

When the EMI indicates that CCI has been set so as to indicate that one generation of copies shall be permitted, the 5C DTCP protocol requires that the content should be encrypted using the 5C system, and that either Restricted or Full Authentication can be performed. The protocol further requires that an authorized copy made from such content shall be marked so as to indicate that no further copies may be made from that copy.

More particularly, the EMI indicates the mode of encryption applied to a stream:

- Licensed source devices will choose the right encryption mode according to the characteristics of the content stream and set its EMI accordingly. If the content stream consists of multiple substreams with different embedded CCI, the strictest embedded CCI will be used to set the EMI.
- Licensed sink devices will choose the right decryption mode as indicated by the EMI.

If the EMI bits are tampered with, the encryption and decryption modes will not match, resulting in an erroneous decryption of the content.

Table 3 shows the encoding used for the EMI bits.

EMI Mode	EMI Value	Meaning	Authentication Required
Mode A	11	Copy-never	Full
Mode B	10	Copy-one-generation	Restricted or Full
Mode C	01	No-more-copies	Restricted or Full
N.A. ⁶	00	Copy freely	None, not encrypted

Table 3. EMI Encoding

⁶ Not Applicable. No EMI mode is defined for an encoding of 00.

The EMI Values have the following meanings:

- An encoding of 00 is used to indicate that the content can be copied-freely. No authentication or encryption is required to protect this content.
- For content that is never to be copied (e.g., content from prerecorded media with a CGMS value of 11), an EMI encoding of 11 is used. This content can only be exchanged between devices that have successfully completed the Full Authentication procedure.
- An EMI encoding of 10 indicates that one generation of copies can be made (e.g., content from prerecorded media with a CGMS value of 10). Devices exchanging this content can either use Full or Restricted Authentication.
- If content with EMI = 10 is copied, future exchanges across a digital interconnect are marked with an EMI encoding of 01, which indicates that a single-generation copy has already been made.

CCI can be transmitted both as EMI and as embedded data. Table 4 shows the CCI value that would be recorded with content programs marked with specific Embedded CCI values.

		Embedded CCI of Program			
		00	01	10	11
EMI	Mode A (Copy-never)	Recordable	Do not record	*	Do not record
	Mode B (Copy-one-generation)	Recordable	Discard entire content stream ⁸	* ⁵	Discard entire content stream
	Mode C (No-more-copies)	Recordable	Do not record	Do not record	Discard entire content stream

Table 4. Format-cognizant Recording Function CCI Handling

Several methods of copy protection have been under discussion in the CPTWG, as well as in working groups of the DVD Forum. These methods include basic marking methods such as CGMS-D and CGMS-A, APS (consisting of the Macrovision analog AGC and colorstripe systems), and methods such as use of watermarks or other embedded data methods to achieve recording control and playback control in compliant devices. The trend of the discussion in the CPTWG clearly anticipates that all of these methodologies may, at some future time, be combined into a comprehensive copy protection methodology capable of securing analog and digital transmissions.

⁷ If the recording function supports recording a CCI value of No-more-copies then the CCI value of No-more-copies shall be recorded with the program. Otherwise the CCI of Copy-never shall be recorded with the program.

⁸ If the function detects this CCI combination among the programs it is recording, the entire content stream is discarded.

transformations among digital formats, conversions between digital and analog formats, and sequential combinations of such conversions. However, it further is clear from the discussions at the CPTWG meetings that a particular methodology using embedded data is not yet ready for selection or implementation in a system for complete protection.

Because it is too early to set in stone the precise means to implement a comprehensive copy protection system that satisfactorily addresses the reasonable concerns of all affected industries, the 5C DTCP system has been designed with sufficient flexibility to accommodate all of these methods. CCI provides the information necessary for the efficient operation of the inexpensive CGMS-D and CGMS-A methods in consumer electronics devices that implement those systems. The CCI similarly provides a method for indicating whether APS is to be activated in content identified as not to be copied, or as first-generation copies that are not further to be copied. Lastly, the 5C specification provides that CCI may be transmitted as embedded data, so that information that has been required to be transmitted as part of the watermark "payload" also may transmit CCI for purposes of protecting against the recording of unauthorized copies of data transmitted using the 5C DTCP system.

Section 8. Resistance to Obsolescence

The resistance of the 5C DTCP system to obsolescence is manifest in several ways.

First, the use of robust 56-bit encryption and Public Key authentication technologies results in a system that will provide sufficient longevity for the devices in which the system is likely to be implemented.

Second, the system of renewability designed by the 5C provides an inexpensive method of isolating and ostracizing devices that are known to be compromised and that create significant potential risks to the system. This renewability is implemented on a device-by-device basis, rather than a system-wide replacement basis. Moreover, device revocation can be rescinded by dissemination of updated Certificate Revocation Lists, which can occur through diverse means that require no effort of the manufacturer or the consumer. Thus, the 5C device-specific revocation results in greater longevity for the 5C system itself and, thus, for the devices that implement the 5C system.

Third, the 5C believes that it would be possible to implement enhancements to the system without disenfranchising existing devices. For example, if longer encryption words become desirable in the future, it should be possible to use both the current 56-bit encryption word and the longer encryption word so that devices that are capable of using the longer encryption word would benefit from the additional level of security, while legacy devices could continue to use 56-bit encryption.

Fourth, as secure bus encryption, the 5C DTCP system provides for interoperability with copy protection technologies that may be introduced in the future. As copy protection technology advances, the 5C DTCP system can continue to provide a secure means of transmitting digital signals that incorporate new watermarking solutions and new forms of content encryption. The 5C DTCP Specification does not limit the development of future recording formats that may utilize advanced techniques of content encryption for recorded media. Discs, tape, flash memory and transmission may require differing methods of handling data. Manufacturers can employ a common 5C DTCP system for secure transmission, and maintain the flexibility to optimize other copy protection technologies for needs of particular formats.

Section 9. Maintenance Complexity

The 5C DTCP system requires minimal, if any, maintenance efforts by consumer electronics manufacturers once devices are first transferred in commerce by the manufacturer.

Key and certificate sets ("device sets") are obtained in advance from a secure key generation facility operated under contract to the DTLA. Device sets can include device keys for Full Authentication, Restricted Authentication, or one set for both Full and Restricted Authentication. The ability to order a set for both Full and Restricted Authentication enables a manufacturer to use the keys required for the particular type of devices being manufactured, and to discard any unused keys. This provides manufacturers with substantial flexibility in the timing and allocation of manufacture of devices that may use only one type of authentication.

Batches of device sets ordered by manufacturers will be provided electronically or on a encrypted using PGP or equivalent public/private key encryption technology to protect the order during transit. Secure installation of certificates in devices is an inexpensive automated process that will add little or no burden to the manufacturing process.

Similarly, storing the initial Certificate Revocation List (CRL) in devices is simple and inexpensive. Updated CRLs will be provided to manufacturers in the same manner as device sets. Propagation of updated CRLs in legacy devices is an automated process that occurs across the home network. Therefore, no effort is required of the manufacturer to update CRLs for existing devices other than installing the most recent CRL in any newly manufactured devices.

Section 10. Applicability to Different Digital Interfaces

The 5C DTCP system can be implemented in any bidirectional interface. Minor modifications may be required for particular interfaces; however, it is believed by the 5C that such modifications will not affect either the effective operation of the 5C DTCP system, or the ability of the system to interoperate across different interfaces.

The 5C further believe that it could be possible to implement the 5C DTCP system on interfaces which support only unidirectional content flow by using an in-band or out-of-band minimal bandwidth back channel for returning information needed to perform functions relating to authentication and key exchange.

The 5C will continue to be open to discuss with any person, on a technical and licensing level, potential methods and APIs that may enable the 5C DTCP system to be used with different technologies or across different interfaces.

Section 11. Availability for Import and Export

Certain elements of the 5C DTCP system require export licensing, including the Hitachi M6 algorithm in a 56-bit implementation and certain aspects of the authentication and key exchange method. All of those elements have been licensed for export by the governments of Japan and the United States. Pursuant to a commodity classification from the United States government, devices incorporating the 5C DTCP system do not require export licenses.

Section 12. Licensing Terms

The 5C DTCP Specification is available for licensing through the Digital Transmission Licensing Administrator (DTLA). The Digital Transmission Licensing Administrator can be contacted at dtla-manager@dtcp.com.

Copies of the nondisclosure agreement and evaluator license for the 5C DTCP system are available directly from the DTLA, and from Digital Transmission Licensing Administrator web site, <http://www.dtcp.com>.

Licenses are available on terms that are demonstrably fair and nondiscriminatory, consistent with the IPR policy of CEMA. The DTLA nondisclosure agreement also is available on terms that are consistent with the NDA policy of CEMA.

License fees for the 5C DTCP system are as follows:

ADOPTER CATEGORY ADMINISTRATION FEES

Small Adopter Fee: \$14,000
Large Adopter Fee: \$18,000
Component Supplier: \$14,000

DEVICE CERTIFICATE AND DEVICE KEY FEES

Small Adopter: \$.06 per device set
Large Adopter: \$.05 per device set

DTLA anticipates that device sets that would enable a manufacturer to implement either Full and Restricted Authentication in a single device will be made available for a total device set fee that is less than would otherwise be charged for two separate device sets.

Section 13. Licensable Intellectual Property

The 5C DTCP system incorporates licensable intellectual property of the 5C member companies. The 5C DTCP Specification uses IP elements from patents issued in the United States, Japan and European countries. Patented aspects of the 5C DTCP Specification include issued and pending patents covering the M6 algorithm, Authentication protocols, EMI, renewability mechanisms, C-CBC, and other elements. The 5C DTCP Specification also incorporates trade secret information of the 5C member companies.

All licenses and immunities from suit for the intellectual property owned by the 5C in the 5C DTCP system are made available in the license from the DTLA.

Section 14. Circumvention Devices

The 5C DTCP system satisfies the generally-accepted standard of the CPTWG that content protection systems should be sufficiently robust against circumvention so as to “keep honest people honest.”

The Hitachi M6 algorithm implemented in the 5C DTCP system is a 56-bit encryption method. To our knowledge, the 5C DTCP system is the first mass-market implementation of 56-bit encryption applied to the delivery of audiovisual digital content across a wide variety of platforms and specifically for consumer electronic and personal computing devices manufactured by a large number of companies. The M6 algorithm has been in commercial use for several years in satellite-based television delivery systems in Japan. To our knowledge it has not been circumvented in that context. The 5C therefore believes that use of M6 in a 56-bit implementation imposes a substantial and robust barrier against unauthorized decryption of protected content.

The Authentication and Key Exchange is performed using the Elliptic Curve Digital Signature Algorithm (EC-DSA) for signing and verification, and the Elliptic Curve Diffie-Hellman (EC-DH) key exchange algorithm to generate a shared authentication key. These methods have been successfully employed widely over the last two decades in a variety of contexts in digital networks requiring secure transmissions and privacy of communications. Again, the 5C is unaware of any instances in which these technologies have been proved to be susceptible to attack or circumvention in commercial application.

The robustness of the system is further enhanced by the ability of the system to change the content keys used to encrypt the content as often as every 30 to 120 seconds, which would require substantial additional effort in circumvention to crack each changed content key.

The 5C system also uses certain shared secrets in CE devices in order to perform restricted authentication in a highly efficient manner. These secrets will be located in silicon (e.g., firmware) in each device. Circumvention in order to discover this secret would require use of professional tools, a commensurately high level of professional skill in the art, and great amounts of time, effort and capital.

Moreover, there is little incentive for piracy of the 5C system because, for the reasons explained below, the “payoff” from circumvention in each case is small.

First, the effect of theft of the secret in a source device is meaningless. Unauthorized reproduction of the device key in a source device would still result in the transmission of content using 5C encryption and authentication, or else the content would not be accepted by compliant sink devices. In such cases, the only losses incurred would be license and certificate fees that otherwise would have been paid to 5C; there would be no damage to content owners whose material is protected using 5C.

Second, theft of the secret in a display sink device would have little consequence for the efficacy of the system. Such devices still would need to comply with the authentication and decryption systems of 5C in order to display protected content. Therefore, cloning of the secret in such a case merely would permit viewing of content using the authentication and encryption protections of the 5C DTCP system. The only loss that would be incurred in the event of such cloning would be the loss of license and certificate fees by the 5C itself.

Third, theft of the secret in a consumer electronics recording device, which would require professional equipment and skills, also is unlikely to result in significant losses or content piracy. Widespread dissemination of such secret could result in revocation of that device certificate and, therefore, disenfranchisement of all rogue devices. For that reason, 5C believes that the threat of revocation will provide a further deterrent against widespread abuse of the system.

Finally, it should be noted that several levels of effective legal remedies are available to deter and to remedy circumvention of the 5C system.

First, as noted above, the 5C DTCP system is protected by patents issued in several countries, including the United States, Europe and Japan, and it is anticipated that additional patents covering the system will be issued by the relevant governmental authorities.

Second, remedies also apply under contract law for violations of the 5C specification by licensees.

Third, trade secret law remedies apply against those who misuse secrets entrusted to them pursuant to the 5C license.

Finally, the 5C system relies on encryption and authentication key exchange means, which would constitute an "effective technological protection measure" pursuant to the terms of newly-enacted 17 U.S.C. § 1201. Thus, circumvention of the system would be subject to effective legal remedies under the Digital Millennium Copyright Act in addition to remedies available for infringement of the intellectual property in the 5C system. This may prove to be the most important legal protection because it has been implemented pursuant to two international treaties approved by more than 120 countries at the World Intellectual Property Organization in December, 1996. To the extent that other countries conclude (as did the United States government) that similar statutory or administrative provisions are required in order to comply with these treaties, statutory protections and effective legal remedies against circumvention will be available on a global basis.

Section 15. Amendments Needed to Interface Standards

The 5C DTCP system complies with existing standards IEEE 1394-1995, IEEE 1394a and IEEE P1363. Required amendments to the AV/C Digital Interface Command Set have been adopted by the 1394TA AV/C Working Group. The current view of the 5C members is that the 5C DTCP system can be implemented using the EIA-775 interface standard without amendment.

The 5C DTCP system in its initial design was not intended for use with unidirectional digital interfaces such as EIA-761 and EIA-762. However, as noted previously, the inclusion of a low bit-rate back channel could be sufficient to permit implementation of a system identical to (or similar to and compatible with) the 5C DTCP system in such unidirectional systems.

Section 16. View of 5C Regarding Standardization of Copy Protection

The 5C believe it is premature for CEMA to attempt standardization of a copy protection system at this time. Discussions in the CPTWG are continuing concerning the elements of a comprehensive system for copy protection. Those discussions have not yet concluded, and are not sufficiently developed so as to permit consumer electronics companies to reach unilateral conclusions as to the minimum necessary elements that will satisfy the needs of (1) those whose content is to be protected, (2) the consumer electronics and information technology industries whose devices will transmit, store and display such content, and (3) consumers who wish to obtain such devices and content.

It is apparent from the CPTWG discussions that any copy protection system determined to be acceptable in concept to all industry participants in the CPTWG process is likely to incorporate some watermark or embedded data solution. Several solutions using different methods currently are under consideration by the CPTWG Data Hiding Subgroup ("DHSG"). According to the general thrust of the CPTWG discussions, watermark or embedded data technology could be used to securely transmit CCI in digital devices, in a manner that could survive several transformations among digital formats and between digital and analog formats. This watermark and embedded CCI also could be used in recording devices to implement methods of copy control, and in playback devices to implement controls against playback of unauthorized copies.

The DHSG participants currently are preparing to enter the next phase of testing, combining an extensive program of self-testing and independent evaluation. It has been recommended that this "Phase 3" DHSG effort should be undertaken under the aegis of the Content Protection Advisory Council ("CPAC") of the CSS Entity. The CSS Entity also has not yet been formed, although such formation is likely to be imminent for purposes of transition from private administration of the CSS system to the Entity. Therefore, the status of both the DHSG work, and the CPAC formation efforts, suggest that standardization by CEMA would be premature.

The DVD Forum WG-9 also is currently investigating a possible system approach to content and copy protection. The progress of their efforts has been described over the last several months to the CPTWG, and has met with substantial interest from the CPTWG members. This project involves individuals from numerous CEMA member companies; however, it is undertaken in the specific context of creating a system that will integrate a system of copy protection originating with signals to and from DVD players, which are the first mass market implementations of consumer electronics digital video products. The WG-9 has established a timeline whereby they are hoping to present their initial conclusions to the CPTWG meeting in January 1999.

The 5C companies further note that companies participating in the CPTWG continue to bring new and innovative copy protection solutions before the group. Any standardization effort, therefore, would reflect only a snapshot in time of technologies that continue to advance and build upon one another.

For all of these reasons, any CEMA process to "standardize" a copy protection solution at this premature stage creates significant risks. First, CEMA members may expend substantial effort toward creating a "standard" that is rendered irrelevant by continuing developments in the CPTWG or CPAC. Second, such standardization efforts could hinder the ongoing CPTWG process if the efforts are based on technologies or assumptions that are not conceptually acceptable to the other industries participating in the CPTWG and CSS Entity processes -- or, indeed, to CE companies that are actively involved in the design, manufacture and marketing of digital video products but are not actively participating in the R4.8 WG2. The 5C believe that such a result would be contrary to the interests of the consumer electronics industry generally, and to the goals articulated by CEMA President Gary J. Shapiro in his letter of October 6, 1998, concerning the intended relationship between the work of this Working Group and the CPTWG.

Finally, the 5C hold the view that it is not necessary to consistently deploy for all consumer electronics devices a unitary technology covering all elements of a comprehensive copy protection solution. Certain aspects of a comprehensive system may differ by product, platform, content type or business model, yet integrate seamlessly with other aspects of the system and, indeed, other systems. To the extent that standardization efforts either might suggest a uniform view that only a single unitary technology is acceptable (or even desirable) for all aspects of a copy protection system, or might thereby hinder development of competing marketplace solutions, the 5C believe that such a standardization effort would be ill-advised and potentially counterproductive.

Section 17. Other Information

In this section, the 5C will address those items, set forth on page 9 of the CFI, which have not previously been addressed in the mandatory sections of this Response.

5. Complexity for Other Industries

The 5C DTCP system has been designed specifically so as to be readily implementable in information technology products, including personal computers, and the next generations of set top boxes that use the Open Cable specification.

Necessary elements of the 5C DTCP system can be integrated into semiconductor devices manufactured under license to the DTLA. Such semiconductor devices are not likely to be specialized semiconductor devices that perform only functionality particular to the 5C DTCP system. Rather, it is a virtual certainty that the necessary functionality for the 5C DTCP system will be integrated into devices that perform other essential functions in each device, such as digital video processing, MPEG-2 decoding, and functions relating to conversion to and from the 1394 interface format. Moreover, based on discussions in the CPTWG and other fora, the 5C believe that technologies that can be incorporated into semiconductor devices and firmware will be acceptable to information technology companies, whereas other types of expensive or external components may not.

The 5C believes that the actual incremental cost of implementing the 5C DTCP system in hardware and software implementation is measured in terms of cents rather than dollars.

12. Consumer Satisfaction

Consumers who use the 5C DTCP system using compliant devices in a manner consistent with the usage authorization rules set forth in the CCI, will be unaware that any protection is being applied to the transmitted content. The latency period for operation of the system is a fraction of a second. The system has no impact on the quality of the audiovisual performance of the protected content. The 5C bus encryption technology also has no effect on features that consumers have come to expect, such as trick playback modes. Consumers thus will be aware of the system only when they attempt to engage in conduct that is contrary to the rules associated with the content. The 5C are endeavoring to ensure that these rules are applied by licensees and content owners in a consistent manner that respects the reasonable expectations of consumers.

Moreover, it is extraordinarily unlikely that any consumer would be affected by revocation of device keys. The 5C anticipate that revocation is most likely to occur in two circumstances, each of which is believed to be unlikely to occur. The first is the improbable case in which a shipment of keys has been intercepted before they have been incorporated into manufactured devices. If this occurs, consumers will not be affected inasmuch as these "lost" keys will not be included in legitimately manufactured devices.

The second is the equally unlikely case in which a single device key from a legitimate consumer electronics device has been hacked, cloned and reproduced en masse into rogue devices. In this case, only the consumer who purchased the legitimate device would be affected by revocation, and it would not be burdensome or expensive for a manufacturer to provide a remedy to that consumer.

13. State of Development of the System

The 5C DTCP Specification has been available for evaluation under a nondisclosure agreement since September 1998. The 5C DTCP system is available now for licensing from the DTLA.

The DTLA has been in operation since September 1998, and has been performing the administrative functions necessary for the rapid adoption and deployment of the 5C DTCP system in the market. Since its inception, the DTLA has executed scores of evaluation nondisclosure agreements with potential licensees, and has issued a number of licenses. Facsimile keys are made available to licensees until the licensees are prepared for commercial manufacture of products.

Under the auspices of the DTLA, a secure facility has been established to generate and distribute device certificates and keys for commercial implementation of the system. These certificate and key sets are being made available to licensees in a secure manner, using PGP encryption.

All necessary licenses from the 5C member companies have been issued to the DTLA to provide licensees with necessary intellectual property rights owned by the 5C members. Export licenses and classifications required to receive the full 5C DTCP Specification and to manufacture and export devices incorporating the 5C DTCP system have been obtained.

[END]

5C Digital Transmission Content Protection

Technical Overview

January 29, 1999

Summary:

- A cryptographic protocol for protecting commercial audio/video entertainment content transmitted across bidirectional digital interfaces against unauthorized interception, tampering and copying.

- any bidirectional interface
- IEEE 1394

Four Basic Elements:

- Authentication and key exchange
- Content encryption
- Copy control information
- System renewability

Authentication and Key Exchange

- Verifies that connected devices are authentic (i.e., that they comply with the 5C DTCP system)
- Two types
 - Full Authentication for “Copy Never” content
 - Restricted Authentication for “Copy One Generation” or “Copy No More” content

Content Encryption

- M6 cipher, using 56-bit encryption
 - developed by Hitachi
– Used in Japan for satellite television broadcasting
- Other ciphers (such as DES, Modified Blowfish) supported as options

Copy Control Information

- Indicates how content is to be treated by receiving device
- Four modes
 - Copy freely (5C DTCP not used)
 - Copy one generation
 - Copy no more
 - Copy never

System Renewability

- If device certificates are cloned and installed in multiple devices
- Individual compromised devices are isolated and ostracized
- Compliant devices will no longer exchange protected content
- Updated revocation list disseminated through multiple sources
- Strict criteria; can be reversed

License Administration

- Digital Transmission Licensing Authority, LLC
 - Issues evaluation agreements, specifications and licenses
 - More than 60 evaluators, several licensees
- Key Generation operational
- Website at <http://www.dtcp.com>

